

Information Security

Objective: The objective of information security is to facilitate business operations and maintain customer services, Agency reputation and revenue while protecting Agency information assets and deeds and other documents belonging to other parties submitted to the Agency from all relevant threats. At all times the cost effectiveness and fitness for purpose of countermeasures will be considered.

Confidentiality: Ensuring that information is accessible only to those authorised to have access

Integrity: Safeguarding the accuracy and completeness of information and processing methods

Availability: Ensuring that authorised users have access to information and associated assets when required

Note : Information takes many forms and can be stored physically or electronically, transmitted across networks or telephone lines, sent by fax, printed as hardcopy or written on paper and spoken in conversations.

INFORMATION SECURITY POLICY STATEMENT

The purpose of the Information Security Policy is to ensure business continuity and minimise business damage by minimising the impact of information security incidents and, where possible, preventing their occurrence.

The Management Board approves and supports the Information Security Policy.

It is the policy of the Agency to ensure that:

- Information will be protected against unauthorised access or misuse.
- Information assets will be classified and protected as required.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Availability of information will be assured.
- Regulatory, legislative and contractual requirements will be met.
- Business continuity plans will be produced, maintained and tested.
- Information security training / instruction will be available to all staff.
- All breaches of electronic information security, actual or suspected will be reported to the Agency IT Security Officer and investigated by the appropriate personnel, and where applicable detail forwarded to the Enterprise Risk Management Forum and the appropriate Government security authorities.

- All breaches of non-electronic information security, actual or suspected, will be reported to management and investigated by the appropriate personnel, and where applicable detail forwarded to the Enterprise Risk Management Forum and the appropriate Government security authorities.
- Standards and procedures will be produced and measures implemented to support the Information Security Policy.
- The Enterprise Risk Manager is responsible for maintaining the Information Security Policy documentation and associated procedures and for providing advice and guidance on their implementation.
- The Departmental Security Officer is accountable for security within the Agency.
- All managers are responsible for implementing the Information Security Policy within their areas of responsibility and for ensuring that their staff are aware of its content.
- It is the responsibility of every employee to comply with the Information Security Policy and apply the guidelines in the Information Security User Guide.
- Infringement of the Information Security Policy will be treated as serious misconduct and will be subject to disciplinary action including dismissal.